Amendment and Response
Applicant: Alexander C. Ranous et al.
Serial No.: 09/560,032
Filed: April 27, 2000
Docket No.: 10002142-1
Title: INTERNET USAGE DATA RECORDING SYSTEM AND METHOD EMPLOYING A CONFIGURABLE RULE ENGINE FOR THE PROCESSING AND CORRELATION OF NETWORK DATA

REMARKS

These remarks are in response to the Non-Final Office Action mailed October 23, 2003. Claims 1-31 were rejected. Claims 1-31 remain pending in the application and are presented for reconsideration and allowance.

Examiner Interview

Applicants' representative thanks the Examiner for the courtesy of a telephone interview on December 23, 2003. Applicants' invention of claim 1 was discussed in view of the cited Bullard reference. The Examiner agreed that details of Applicants' processing the network accounting data set via the aggregator, as detailed in the dependent claims such as claim 4, are not disclosed in Bullard. The Examiner also agreed that claims 30 and 31 are allowable over Bullard.

As a result of the discussion, the Examiner agreed to remove the Finality of the Office Action mailed October 23, 2003. Applicants agreed to respond to the October 23, 2003 Office Action, without amending any claims, to allow the Examiner to reconsider his response to the entire claim set.

Applicant thanks the Examiner for reconsidering all of pending claims 1-31.

Claim Rejections under 35 U.S.C. § 102

Claims 1-11 and 13-29 and 30-31 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,405,251 issued to Bullard et al. (hereinafter Bullard). Applicant submits that the Bullard reference fails to disclose the invention of independent claims 1, 13, 17, 20, 26 and 30.

Independent claim 1 recites a method for recording network usage. The method comprises defining a network data collector including an encapsulator, an aggregator, and a data storage system. A set of network accounting data is received via the encapsulator. A network accounting data set is converted to a standard data format. The network accounting data set is processed via the aggregator, including defining a rule chain and applying the rule

chain to the network accounting data set to construct an aggregation tree including creating an aggregated network accounting data set. The aggregated network accounting data set is stored in the data storage system.

Bullard discloses a system for enhancement of network accounting records. The system includes a data collector layer 18 that is a distributed layer of individual data collectors. The data collectors collect raw accounting information and convert data into normalized records referred to as network accounting records (NARs). Each of the data collectors forwards network accounting records to a flow aggregation process 60. (See column 3, lines 43-54). The flow aggregation process 60, including aggregation processor 13, is a central collection point for all network accounting records produced from various data collectors in the data collection layer 18. The flow aggregation processor 60 aggregates and/or enhances record data across the network devices to produce summary NARs' (column 4, lines 1-26), and (column 18, lines 39-49). The data can be further enhanced and/or reduced (i.e., aggregated) to meet the specific needs of an application or output interface based on the aggregation policy of the flow data processor 60.

Bullard fails to disclose **defining a network data collector including an encapsulator, an aggregator, and a data storage system, where a network accounting data set is processed at the network data collector via the aggregator, including defining a rule chain and applying the rule chain to the network accounting data set to construct and aggregation tree including creating an aggregated network accounting data set.** In contrast, Bullard discloses individual data collectors that collect data and convert data into NARs. The NARs are forwarded to a central flow aggregation processor 13, not part of the data collectors. Although Bullard states that "individual data collectors 52a-52g can aggregate accounting records from individual data sources" (Col. 4, lines 24, 25), Bullard fails to disclose an aggregation process at each collector that applies a rule chain and constructs an aggregation tree as claimed by Applicant.

Bullard does not teach or suggest these claimed recitations. The method for recording network usage of independent claim 1 is not disclosed in Bullard. Applicants respectfully submit that the above rejection under 35 U.S.C. 102(e) should be withdrawn.

Dependent claims 2-12 depend directly or indirectly upon independent claim 1. Accordingly, dependent claims 2-8 are also allowable over the art of record.

Bullard also does not teach or suggest the claimed recitations in independent claim 13. Claim 13 recites a method for recording network usage including correlating of network usage information and network session information. The method includes defining a network data correlator collector including an encapsulator, an aggregator, and a data storage system. A set of network session data is received via the encapsulator. The network session data set is processed via the aggregator, including the steps of defining a first rule chain and applying the first rule chain to the network session data to construct an aggregation tree. A set of network usage data is received via the encapsulator. The network usage data set is processed via the aggregator, including the steps of defining a second rule chain and applying the second rule chain to the network usage data and the aggregation tree to construct a correlated aggregation tree. A correlated data set is determined from the correlated aggregation tree. The correlated data set is stored in the data storage system. Bullard does not teach or suggest these claimed recitations.

Bullard fails to define **a network data correlator collector that includes an encapsulator, an aggregator, and a data storage system.** Bullard further fails to recite **processing a network session data set via the aggregator, including the steps of defining a first rule chain and applying the first rule chain to the network session data to construct an aggregation tree, and processing a network usage data set via the aggregator including defining a second rule chain and applying the second rule chain to the network usage data and the aggregation tree to construct a correlated aggregation tree.** Bullard merely teaches that a number of fields can be captured in a NAR, which in turn can be combined and used to form a summary NAR. (See column 8, table 1).

Dependent claims 14-16 depend directly or indirectly upon independent claim 13. Accordingly, dependent claims 14-16 are also allowable over the art of record.

Bullard also does not teach or suggest the claim recitations in independent claim 17. Claim 17 recites a method for recording network usage. The method includes defining a first network data collector including a first encapsulator, a first aggregator, and a first data storage system. A first set of network data is received via the first encapsulator. The first

network data set is processed via the first aggregator, including the steps of defining an aggregation rule chain in determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data. The first aggregated network data set is stored in the first data storage system. Bullard does not teach or suggest these claimed recitations. Applicant respectfully submits that the above rejection under 35 U.S.C. 102(e) should be withdrawn. Dependent claims 18 and 23 depend directly or indirectly upon independent claim 17. Accordingly, these dependent claims are allowable over the art of record.

Bullard also does not teach or suggest the claimed recitations in independent claim 24. Claim 24 recites a network usage recording system having a network data collector. The network data collector includes an encapsulator for receiving a set of network accounting data and converting the network accounting data set to a standard data format. An aggregator processes the network accounting data set, the aggregator including a defined rule chain, wherein the aggregator applies the rule chain to the network accounting data set to construct an aggregation tree, and determines a set of aggregated network accounting data from the aggregation tree. A data storage system stores the aggregated network accounting data. Bullard does not teach or suggest these claimed recitations. Applicant respectfully submits that the above rejection under 35 U.S.C. 102(e) should be withdrawn.

Dependent claim 25 depends directly upon independent claim 24. Accordingly, this dependent claim is allowable over the art of record.

Bullard also does not teach or suggest the claimed recitations in independent claim 26. Claim 26 recites a network usage recording system having a network data correlator collector. The network data correlator collector includes an encapsulator which receives a set of network session data. An aggregator for processing the network session data set, the aggregator including a defined first rule chain wherein the aggregator applies the first rule chain to the network session data set to construct an aggregation tree. The encapsulator receives a set of network usage data, and the aggregator processes the network usage data set, the aggregator including a defined second rule chain, wherein the aggregator applies the second rule chain to the network usage data set and the aggregation tree to construct a correlated aggregation tree, and determines a correlated data set from the correlated

aggregation tree. A data storage system stores the correlated data set. Bullard does not teach or suggest these claimed recitations. Applicant respectfully submits that the above rejection under 35 U.S.C. 102(e) should be withdrawn.

Dependent claims 27-29 depend either directly or indirectly upon independent claim 26. Accordingly, these dependent claims are allowable over the art of record.

Bullard also does not teach or suggest the claimed recitations in independent claim 30. Claim 30 recites defining a first network data collector including a first encapsulator, a first aggregator, and a first data storage system. A first set of network data is received via the first encapsulator. The first network data set is processed via the first aggregator, including defining an aggregation rule chain and determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data. The first aggregated network data set is stored in the first data storage system.

Applying the aggregation rule chain to the first set of network data further comprises constructing an aggregation tree. The first aggregated network data set is determined from the aggregation tree, where constructing an aggregation tree includes defining the first network data set to include a first network data event and a second network data event. The aggregation rule chain is applied to the first network data event to construct a hierarchy of group nodes within the aggregation tree. The aggregation rule chain is applied to the second network data event to locate similar group nodes according to a predefined set of match rules, if no matching group nodes exist, the hierarchy of group nodes is extended within the aggregation tree by creating additional group nodes.

Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule chain to include a first match rule for matching source IP address. The first network data event is defined to include a first source IP address. The first match rule is applied to the first network data event, including determining whether the aggregation tree includes a first group node matching the first source IP address, and if a matching first group node does not exist, creating the first group node for the first source IP address.

Applying the aggregation rule chain to the first network data event includes defining the aggregation rule chain to include a second match rule for matching destination IP address.

The first network data event is defined to include a first destination IP address. The second match rule is applied to the first network data event, including determining whether the aggregation tree includes a second group node matching the first destination IP address, and if a matching second group node does not exist, creating the second group node for the first destination IP address. Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule set to include an aggregation rule. The first network data event is defined to include a port number and volume of information. The aggregation rule is applied to the first network data event, including copying the port number, source IP address, destination IP address and volume information to the second group node. Bullard does not teach or suggest these claimed recitations. Applicant respectfully submits that the above rejection under 35 U.S.C. 102(e) should be withdrawn. Dependent claim 31 depends directly upon independent claim 30. Accordingly, this dependent claim is allowable over the art of record.

Rejections under 35 U.S.C. §103

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bullard in view of U.S. Patent No. 6,199,195 issued to Goodwin et al. Dependent claim 12 depends directly upon independent claim 1. Accordingly, dependent claim 12 is also allowable over the art of record.

CONCLUSION

In light of the above, Applicant believes independent claims 1, 13, 17, 20, 26 and 30 and the claims depending therefrom, are in condition for allowance. Allowance of these claims is respectfully requested.

Any inquiry regarding this Amendment and Response should be directed to either Philip S. Lyren at Telephone No. (281) 514-8236, Facsimile No. (281) 514-8332 or Steven E. Dicke at Telephone No. (612) 573-2002, Facsimile No. (612) 573-2005. In addition, all correspondence should continue to be directed to the following address:

Amendment and Response
Applicant: Alexander C. Ranous et al.
Serial No.: 09/560,032
Filed: April 27, 2000
Docket No.: 10002142-1
Title: INTERNET USAGE DATA RECORDING SYSTEM AND METHOD EMPLOYING A CONFIGURABLE RULE ENGINE FOR THE PROCESSING AND CORRELATION OF NETWORK DATA

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Respectfully submitted,

Alexander C. Ranous et al.,

By their attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2002
Facsimile: (612) 573-2005

Date: December 23, 2003
SED:jan

Steven E. Dicke
Reg. No. 38,431

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this paper or papers, as described herein, are being facsimile transmitted to the United States Patent and Trademark Office, Fax No. (703) 872-9306 on this 23rd day of December, 2003.

By Steven E. Dicke
Name: Steven E. Dicke